UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/609,508	06/30/2003	David I. Poisner	042390.P16204	1159

45209 7590 11/27/2007
INTEL/BLAKELY
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
11/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/609,508	**Applicant(s)** POISNER, DAVID I.	
	Examiner Minh Dieu Nguyen	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 September 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,13,15,16 and 32-34* is/are pending in the application.

4a) Of the above claim(s) *2,3,5-12,14 and 17-31* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,13,15,16 and 32-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10/5/2007*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to the communication dated 9/11/2007 with the amendments to claims 1, 4, 13 and 15-16, the addition of claims 32-34 and the cancellation of claims 2-3, 5-12, 14, 17 and 21-31.

2. Claims 1, 4, 13, 15-16 and 32-34 are pending.

Response to Arguments

3. Applicant's arguments dated 9/11/2007 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. Claims 1, 16 and 32-33 are objected to because of the following informalities:

a) As to claim 1, "an SRAM (synchronous random access memory)" is recited, however the specification, paragraph 0019 discloses dynamic random access memory (DRAM). Synchronous dynamic random access memory (SDRAM) is other type of DRAM. As such, "an SRAM (synchronous random access memory)" should be changed to "**a synchronous dynamic random access memory (SDRAM)**".

b) As to claim 16, the phrase "the protected register" should be **"protect register"**.

c) As to claims 32 and 33, the phrase "decrypting the data" should be changed to "decrypting the **received** data".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 13, 15 and 34 are rejected under 35 U.S.C. 102(e) as being anticipated by England et al. (2004/0003262).

a) As to claim 13, England discloses a chipset (i.e. USB security module, England: Fig. 1, element 702) comprising: a host controller to transmit an encryption key to a peripheral device (i.e. key service processor 708 of the USB security module 702 can provide an interface that can be called using a secure channel to set up which devices are secured and what the proper key(s) for the device should be, England: 0059, Fig. 1, and the USB security module 702 could be located at a USB device or function, an in-line device or "dongle", a USB hub, or the USB Host Controller, England: 0062); receive data from the peripheral device (i.e. if the data is enroute from a USB device and is intended for a secure application, then the data can be encrypted and subsequently provided to the application and/or into memory, England; 0061) and if the received data is data encrypted based, at least in part, on the encryption key, the host controller to enable use of a peripheral software stack associated with the peripheral device to process data transmitted from the peripheral device (i.e. USB systems have been secured can allow an encrypted tunnel to be established through an unmodified USB tree, and for the most part, an unmodified USB device-driver stack. The tunneling can happen in both directions...In the input direction, a secure application can obtain key strokes, mouse packets, secure biometric data, microphone data, and the like from USB devices, England: 0032).

b) As to claim 15, England discloses the chipset of claim 13, wherein the encryption key is received from a CPU coupled to the chipset (i.e. the USB security module, England: Fig. 1, elements 702) should reside in the USB Host Controller or on the motherboard (e.g. CPU is built in), England: 0063).

c) As to claim 34, England discloses a chipset of claim 13, wherein the encryption key is received from the peripheral device (i.e. the USB security module 702 could be located at a USB device or function, an in-line device or "dongle", a USB hub, or the USB Host Controller, England: 0062, as such, the encryption key is generated at the peripheral device since the USB security module can be incorporated into device hardware).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

> the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 4, 16 and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over England et al. (2004/0003262) in view of Patariu et al. (2004/0247129).

a) As to claim 1, England discloses a computer system (i.e. computing system comprising one or more processors, a system memory and a bus that couples various system components including the system memory to the processor, England: 0039) comprising: an SRAM (synchronous random access memory) to store trusted software (i.e. RAM 210 typically contains data (e.g. operating system) and/or program modules that are immediately accessible to and/or presently be operated on by processing unit 202, England: 0042, 0045); the chipset additionally having a host controller to transmit the encryption key to a peripheral device (i.e. key service processor 708 of the USB security module 702 can provide an interface that can be called using a secure channel to set up which devices are secured and what the proper key(s) for the device should be, England: 0059, Fig. 1, and the USB security module 702 could be located at a USB device or function, an in-line device or "dongle", a USB hub, or the USB Host Controller, England: 0062) and receive data from the peripheral device (i.e. if the data is enroute from a USB device and is intended for a secure application, then the data can be encrypted and subsequently provided to the application and/or into memory, England; 0061) and if the received data is data encrypted based, at least in part, on the encryption key, the host controller to enable use of a peripheral software stack associated with the peripheral device to process data transmitted from the peripheral device (i.e. USB systems have been secured can allow an encrypted tunnel to be established through an unmodified USB tree, and for the most part, an unmodified USB device-driver stack. The tunneling can happen in both directions...In the input direction, a secure application can obtain key strokes, mouse packets, secure biometric data, microphone data, and the like from USB devices, England: 0032).

England is silent on the capability of having the trusted software to write an encryption key to protected registers in a chipset.

Paratiu is relied on for the teaching of having the trusted software to write an encryption key to protected registers in a chipset (i.e. a memory (DRAM) 104 may be coupled to the bus interface block, under control of suitable hardware and/or software, the key generator/controller block may be adapted to generate one or more key values, ..., the association and transfer of the serially transmitted keys via the serial bus may include writing and storing the serially transmitted keys to one or more key registers, England: 0027, 0042).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the trusted software to write an encryption key to protected registers in a chipset in the system of England, as Paratiu teaches, so as to provide a secure access and processing of an encryption/decryption key (Paratiu: 0008)..

b) As to claim 4, the combination of England and Paratiu discloses the system of claim 1, wherein the trusted software writes to the protected registers to indicate to the host controller the encryption key to transmit and response data that is to be received from the peripheral device (i.e. serially transmitted keys are written and stored to one or more key registers, and encrypted data stored in the external data processing/storage device 116 may be transferred from the external data processing/storage device 116 for decryption by the encryption/decryption processor block 114, wherein the first bus connecting to external data processing/storage device is a USB bus, Paratiu: 0042, 0032, 0026).

c) As to claim 16, England discloses the chipset of claim 13, however he is silent on the capability of having trusted software writes an encryption key to the protected registers to indicate to the host controller the encryption key to transmit and response data that is to be received from the peripheral device.

Paratiu is relied on for the teaching of having trusted software writes an encryption key to the protected registers to indicate to the host controller the encryption key to transmit and response data that is to be received from the peripheral device (i.e. serially transmitted keys are written and stored to one or more key registers, and encrypted data stored in the external data processing/storage device 116 may be transferred from the external data processing/storage device 116 for decryption by the encryption/decryption processor block 114, wherein the first bus connecting to external data processing/storage device is a USB bus, Paratiu: 0042, 0032, 0026).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having trusted software writes an encryption key to the protected registers to indicate to the host controller the encryption key to transmit and response data that is to be received from the peripheral device in the system of England, as Paratiu teaches, so as to provide a secure access and processing of an encryption/decryption key (Paratiu: 0008).

d) As to claim 32, the combination of England and Paratiu discloses the system of claim 1, wherein an operating system determines if the received data is data encrypted based, at least in part, on the encryption key by: decrypting the data; comparing the decrypted data to the expected response data, and if the decrypted data matches the expected response data, determining that the received data is encrypted based, at least in part, on the encryption key (i.e. decrypting data and verifying the data to protect the integrity of data that is provided onto the USB, England: 0080-0084, the fact that the received data can be decrypted, it anticipates the received data is encrypted based on the encryption key).

e) As to claim 33, the combination of England and Paratiu discloses the chipset of claim 16, wherein an operating system determines if the received data is data encrypted based, at least in part, on the encryption key by: decrypting the data; comparing the decrypted data to the expected response data, and if the decrypted data matches the expected response data, determining that the received data is encrypted based, at least in part, on the encryption key (i.e. decrypting data and verifying the data to protect the integrity of data that is provided onto the USB, England: 0080-0084, the fact that the received data can be decrypted, it anticipates the received data is encrypted based on the encryption key).

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MinhDieu Nguyen
Patent Examiner
11/21/07